NEWS RELEASE

OFFICE OF THE UNITED STATES ATTORNEY
WESTERN DISTRICT OF MISSOURI

TODD P. GRAVES

Contact Don Ledford, Public Affairs ● (816) 426-4220 ● 400 East Ninth Street, Room 5510 ● Kansas City, MO 64106
www.usdoj.gov/usao/mow

APRIL 8, 2004
FOR IMMEDIATE RELEASE

BELTON MAN INDICTED FOR HACKING INTO FORMER EMPLOYER'S COMPUTER DATABASE

KANSAS CITY, Mo. – Todd P. Graves, United States Attorney for the Western District of Missouri, announced that a Belton, Mo., man was indicted by a federal grand jury today for computer hacking.

Christopher W. Jones, 28, of Belton, was charged in an indictment returned by a federal grand jury in Kansas City.

The federal indictment alleges that **Jones** knowingly and without authorization caused the transmission of a computer command that resulted in intentional damage to a protected computer, causing a loss of at least $5,000 during the one year period following Aug. 21, 2003.

The protected computer was that of his former employer Relate, LCC, d.b.a. Event Photographers Online. **Jones'** employment with Event Photographers Online had been terminated on Aug. 21, 2003, after no agreement with the company could be reached regarding **Jones'** future compensation. **Jones** had been employed with the company since January 2002. He was responsible for maintaining and developing the company's Web site and, therefore, was provided access to Event Photographers Online's computer database.

The federal indictment alleges that after being terminated from the company, **Jones** accessed Event Photographers Online's computer database on three occasions from his home computer over a 12-hour period.

The federal indictment alleges that the first unauthorized access session was initiated at 8:22 p.m., on Aug. 21, 2003, when **Jones** logged on to the site as user "epo 331," and uploaded a number of "active server pages." The files were named "noonan.asp," "email.asp," "admin.asp," and "choose.asp." These files copied information in the database and returned it to **Jones** and deleted specific files and information contained in the database, the indictment alleges.

The federal indictment alleges that the second unauthorized access session was initiated at 1:39 a.m., on Aug. 22, 2003. During the second unauthorized session, **Jones** initiated delete commands as to 83 individual items from the company's Web site and computer database, the indictment alleges. As a result, the Web site was disabled, denying the company's customers access to its content. Company officials also lost their ability to access the Web site.

The federal indictment alleges that the third unauthorized access session was initiated at 8:15 a.m., on Aug. 22, 2003. During the third session, **Jones** uploaded the "noonan.asp," and "admin.asp," a second time after he had modified the files. The files again acted as malicious scripts and deleted or wrote over additional records contained in the company's computer database. On this occasion, the Web hosting company engineer discovered that there was an intruder actively accessing the Web site and database.

Graves cautioned that the charges contained in the indictment are simply accusations, and not evidence of guilt. Evidence supporting the charges must be presented to a federal trial jury, whose duty is to determine guilt or innocence.

The case is being prosecuted by Assistant U.S. Attorney Curt Bohling. It was investigated by the Federal Bureau of Investigation.

****

This news release, as well as additional information about the office of the United States Attorney for the Western District of Missouri, is available on-line at
www.usdoj.gov/usao/mow